

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平8-106436

(43) 公開日 平成8年(1996)4月23日

(51) Int. Cl. ⁶

G06F 15/00

識別記号

330

庁内整理番号

B 9364-5L

F I

技術表示箇所

審査請求 未請求 請求項の数 2 O L (全7頁)

(21) 出願番号 特願平6-238672

(22) 出願日 平成6年(1994)10月3日

(71) 出願人 000005223

富士通株式会社

神奈川県川崎市中原区上小田中1015番地

(72) 発明者 田中 振一郎

神奈川県川崎市中原区上小田中1015番地

富士通株式会社内

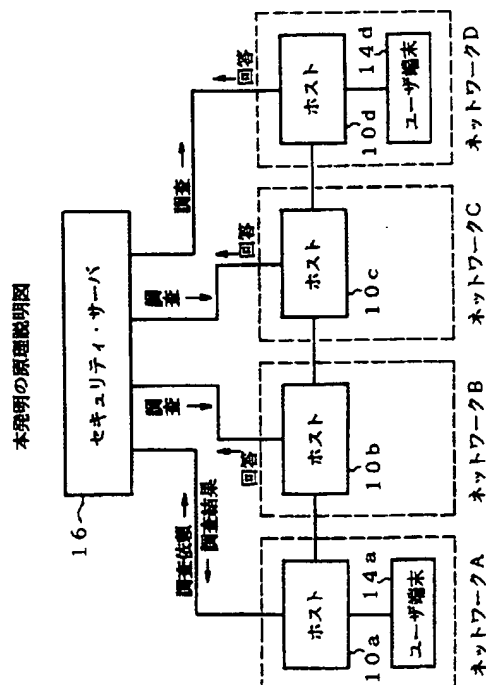
(74) 代理人 弁理士 竹内 進 (外1名)

(54) 【発明の名称】 広域ネットワークのユーザ認証装置

(57) 【要約】

【目的】 複数ネットワークのホストコンピュータを経由して不正利用しているユーザ端末を調査可能とする。

【構成】 複数のネットワークA～Dに設けた各ホストコンピュータ10a～10dに対しセキュリティ・サーバ16を接続し、各コンピュータ10a～10dからのユーザ調査依頼に対しセキュリティ・サーバ16が他のホストコンピュータのユーザ接続情報を参照して発信元のユーザ端末14dを調査する。



【特許請求の範囲】

【請求項 1】ホストコンピュータとユーザ端末を備えた複数のネットワークを相互に接続し、各ネットワークのユーザ端末から他のネットワークのユーザ端末にログインして情報を送受する広域ネットワークに於いて、前記複数のネットワークに設けた各ホストコンピュータと接続し、各コンピュータからのユーザ調査依頼に対し他のホストコンピュータのユーザ接続情報を参照して発信元のユーザ端末を調査するセキュリティ・サーバを設けたことを特徴とする広域ネットワークのユーザ認証装置。

【請求項 2】請求項 1 記載の広域ネットワークのユーザ認証装置に於いて、前記各ネットワークのホストコンピュータは、他のネットワークを経由したユーザ端末からのログインに対し、前記セキュリティ・サーバにユーザ調査依頼を行い、該調査結果に基づいて前記ログインを許可又は拒否することを特徴とする広域ネットワークのユーザ認証装置。

【発明の詳細な説明】

【0001】

【産業上の利用分野】本発明は、複数のコンピュータネットワークをお互いに結んだインターネットとして知られた広域ネットワークのユーザ認証装置に関する。

【0002】

【従来の技術】従来、企業や大学の研究機関などのネットワークは、大型のホストコンピュータを中心に多数の端末機器を接続したローカルエリア・ネットワークとして構築されていたが、近年、このようなコンピュータネットワークをお互いに接続した広域ネットワークがインターネットとして急速に普及してきている。現在のところ、世界中の三百万台のコンピュータからなる 3 万のネットワークが存在するといわれ、これらのネットワークを相互に結合することで、極めて利用価値の高いネットワークが構築可能となる。

【0003】図 4 は、広域ネットワークの一例であり、4 つのネットワーク A ～ D を相互に結合しており、各ネットワーク A ～ D には、ホストコンピュータ 10 a ～ 10 d と、複数のユーザ端末が設けられる。そして、インターネットとしてネットワーク A ～ D を相互に結合することで、例えばネットワーク D のユーザ端末 14 d からネットワーク C、B を経由してネットワーク A のユーザ端末 14 a にログインして、情報のやり取りを行うことができる。

【0004】

【発明が解決しようとする課題】ところで、インターネットとしての広域ネットワークを構築した場合、他のネットワークからの通信要求を全て受け入れると、ネットワーク内部での情報のやり取りが制限される。そこで、各ネットワークにあっては、他のネットワークからログイン可能なユーザ端末の数に制限を加える場合がある。

【0005】またネットワークによっては、特定のユーザ端末の情報については有料とする場合もあり、この場合には、ユーザ ID を知って課金処理を行うことになる。このため広域ネットワークの中でコンピュータを運用していくに当たっては、セキュリティの強化が重要になる。しかし、広域ネットワーク上で特定のネットワークに不正にログインしようとするユーザ端末が、他の複数のネットワークを経由して侵入してきた場合、どこのネットワークのユーザ端末から侵入してきたかの追跡は、現状では不可能に近いという問題がある。

【0006】例えば図 5 のように、ネットワーク D のユーザ端末 14 d からネットワーク A のユーザ端末 14 a に不正にログインを行ったとする。このログインは、ネットワーク D ～ A のホストコンピュータ 10 d、10 c、10 b、10 a を経由して来る。このユーザ端末 14 a に対するログインが不正利用と判っても、ホストコンピュータ 10 a へのログインは、ネットワーク B のホストコンピュータ 10 b に接続している仮想的なユーザ端末 14 b からのログインとしてしか見えず、ネットワーク C からのログインであることは判らない。同様にネットワーク B のホストコンピュータ 10 b から見たログインは、ネットワーク C のホストコンピュータ 10 c に接続している仮想的なユーザ端末 14 c からのログインとしてしか見えず、ネットワーク D からのログインであることは判らない。

【0007】この場合、ホストコンピュータ 10 a からホストコンピュータ 10 b、10 c に、ユーザ端末との接続状況を問い合わせればよい。しかし、ホストコンピュータ 10 b、10 c は各々が独立した固有のネットワーク B、C を構築しているため、ホストコンピュータ 10 a からの問い合わせに協力的であるとは限らない。このため複数のネットワークのホストコンピュータを経由した不正なログインは、現在の広域ネットワークでは調べようがなく、不正なログインをそのまま見逃してしまう問題がある。

【0008】本発明は、このような従来の問題点に鑑みてなされたもので、複数ネットワークのホストコンピュータを経由して不正利用しているユーザ端末を調査して必要な措置がとれるようにした広域ネットワークのユーザ認証装置を提供することを目的とする。

【0009】

【課題を解決するための手段】図 1 は本発明の原理説明図である。まず本発明は、ホストコンピュータ 10 a ～ 10 d とユーザ端末 14 a、14 d を備えた複数のネットワーク A ～ D を相互に接続し、各ネットワークのユーザ端末から他のネットワークのユーザ端末にログインして情報を送受する広域ネットワークを対象とする。

【0010】このような広域ネットワークのユーザ認証装置として、本発明にあっては、複数のネットワーク A ～ D に設けた各ホストコンピュータ 10 a ～ 10 d と接

続し、各コンピュータ 10 a ~ 10 d からのユーザ調査依頼に対し他のホストコンピュータのユーザ接続情報を参照して発信元のユーザ端末 14 d を調査するセキュリティ・サーバ 16 を設けたことを特徴とする。

【0011】ここで、各ネットワーク A ~ D のホストコンピュータ 10 a ~ 10 d は、他のネットワークを経由したユーザ端末からのログイン、例えばネットワーク C、B を経由したネットワーク D のユーザ端末 14 d からネットワーク A のホストコンピュータ 10 a へのログインに対し、セキュリティ・サーバ 16 にユーザ調査依頼を行い、調査結果に基づいてログインを許可又は拒否する。

【0012】

【作用】このような本発明の広域ネットワークのユーザ認証装置によれば、複数のネットワークを経由したログインの情報を、各ホストコンピュータの上位に位置するセキュリティ・サーバで参照することで、ネットワークを越えて不正にログインしているユーザ端末装置を認識することができ、広域ネットワークのセキュリティを高めることができる。

【0013】

【実施例】図 2 は、本発明のユーザ認証装置が適用される広域ネットワークの一例である。図 2 において、この実施例にあつては、4 つのネットワーク A、B、C、D で広域ネットワークを構成している。即ち、ネットワーク A ~ D のそれぞれにはホストコンピュータ 10 a、10 b、10 c、10 d が設けられ、ホストコンピュータ 10 a ~ 10 d は、お互いに通信回線 12 で接続されている。

【0014】ここで、ホストコンピュータ 10 a ~ 10 d を通信回線 12 で直直接接続しているが、これは図示の都合であり、実際にはホストコンピュータ 10 a ~ 10 d が相互に通信回線 12 で接続されている。ホストコンピュータ 10 a ~ 10 d のそれぞれには、ネットワーク内部のローカルエリア・ネットワークによって複数のユーザ端末が接続されている。

【0015】ネットワーク A ~ D 内でのユーザ端末間の通信は、例えばネットワーク A を例にとると、ユーザ端末 14 a が、ネットワーク内の他のユーザ端末に対する通信のためホストコンピュータ 10 a に対し予め定めたパスワードとユーザ ID を送ることによってログインすることができる。このログインにあつては、発信元となるユーザ端末 10 a より、相手先を示すユーザ ID が同時に送られる。

【0016】一方、異なるネットワークのユーザ端末間での通信については、その間に存在する複数のホストコンピュータを経由したログインが行われる。例えば、ネットワーク D のユーザ端末 14 d からネットワーク A のホストコンピュータ 10 a にログインしてユーザ端末 10 a と通信したい場合には、ユーザ端末 14 d からホス

トコンピュータ 10 d に対するログイン、ホストコンピュータ 10 d からホストコンピュータ 10 c に対するログイン、ホストコンピュータ 10 c からホストコンピュータ 10 b に対するログインを経て、ホストコンピュータ 10 a に対するログインが行われる。

【0017】この場合、ユーザ端末 10 d はネットワーク A のホストコンピュータ 10 a について定められたパスワードと自分自身のユーザ ID を送ってログインを行う。ユーザ端末 10 d からのログインに基づくホストコンピュータ 10 d からホストコンピュータ 10 a へのログインの伝送は、ユーザ端末 14 d が発信したパスワードを解析して、ネットワーク A に対するログインであることを認識して、次のネットワークのホストコンピュータに送り出すようになる。したがって、ネットワーク D とネットワーク A の間に存在するネットワーク C、B のホストコンピュータ 10 c、10 b には、ログインが行われたユーザ端末 10 d からの送信情報が記録保持されている。

【0018】このような 4 つのネットワーク A ~ D のホストコンピュータ 10 a ~ 10 d に対しては、共通にセキュリティ・サーバ 16 が接続される。セキュリティ・サーバ 16 は、ホストコンピュータ 10 a ~ 10 d からのログインしてきたユーザ端末に関する調査依頼を受けると、調査対象となったユーザ端末の発信元から発信先の間に位置するネットワークのホストコンピュータに対し、調査対象となったユーザ端末に関する調査を依頼する。具体的には、ホストコンピュータに対し、調査対象となっているユーザ端末のパスワードと ID コードを提供して、その通信記録を読み出して回答させる。

【0019】例えば図 2 のように、ネットワーク D のユーザ端末 14 d よりネットワーク A のホストコンピュータ 10 a がログインを受けた場合、この外部からのログインが、どのネットワークのユーザ端末によるものか判らないことから、ホストコンピュータ 10 a はセキュリティ・サーバ 16 に対し、ログインしたパスワードとユーザ ID を指定したユーザ端末の調査を依頼する。

【0020】ホストコンピュータ 10 a からの調査依頼を受けたセキュリティ・サーバ 16 は、他の全てのホストコンピュータ 10 b、10 c、10 d に対しパスワードとユーザ ID を提供し、調査を依頼する。セキュリティ・サーバ 16 からの調査指示を受けたホストコンピュータ 10 b ~ 10 d のそれぞれは、その通信記録を読み出してセキュリティ・サーバ 16 に回答する。

【0021】具体的には、ホストコンピュータ 10 b は、調査対象となったパスワードおよびユーザ ID のユーザ端末はネットワーク C のホストコンピュータ 10 c からのログインであることを回答する。またホストコンピュータ 10 d は、調査対象となったパスワードおよびユーザ ID のログインはネットワーク D のホストコンピュータ 10 d からのログインであったことを回答する。

10

20

30

40

50

更にホストコンピュータ10dは、調査対象となったパスワードとユーザIDのログインは自分のネットワーク内のユーザ端末10dからのログインであったことを回答する。

【0022】このようなホストコンピュータ10b～10dからの調査指示に対する回答結果をセキュリティ・サーバ16で解析すると、ホストコンピュータ10aから調査依頼があったパスワードとユーザIDのログインは、ネットワークDのユーザ端末14dから行われたものであることが判り、この調査結果をホストコンピュータ10aに回答する。これによって、ホストコンピュータ10a側において、調査対象としたログインがネットワークDのユーザ端末14dから行われていることを認識できる。

【0023】一方、セキュリティ・サーバ16による追跡調査でユーザ端末が突き止められず、追跡不能との調査結果の回答を受けた場合には、ホストコンピュータ10aにおいて、調査対象としたユーザ端末のログインを拒否することもできる。図3は、図2の各ホストコンピュータ10a～10dにおけるセキュリティ・サーバ16を利用したセキュリティ処理のフローチャートである。

【0024】まずステップS1で、必要があれば、調査対象となるユーザIDを予め設定しておく。この調査対象のユーザIDの設定状態で、ステップS2でログインをチェックしており、ログインがあると、ステップS3で、パスワードとユーザIDをチェックし、ステップS4で、調査対象として設定したユーザが否かチェックする。

【0025】ログインしてきたユーザが調査対象として設定したユーザであった場合には、ステップS5で、セキュリティ・サーバ16に対しパスワードとユーザIDを通知して、ユーザ端末の調査を依頼する。この調査依頼を受けて、セキュリティ・サーバ16は他のホストコンピュータに調査を指示し、その回答から調査対象となったユーザ端末の追跡結果を報告してくる。この調査結果は、ステップS6で受信される。

【0026】調査結果からユーザ端末が追跡できていた場合には、ステップS7からステップS8に進み、調査したユーザIDをもつユーザ端末を記録し、ユーザ端末が判っていることから、ステップS9で、ログインを受

領する。また、調査したユーザ端末が不正使用であった場合には、ステップS8の記録結果を利用して、追跡したユーザ端末の不正使用に対し必要な措置をとることができる。

【0027】一方、ステップS7で、受信した調査結果からユーザ端末が追跡不能であった場合には、ステップS10で、ログインを拒否する。即ち、セキュリティ・サーバ16で追跡不能のようなユーザ端末は、本来、不正使用を意図していることが明らかであることから、ログイン自体を拒否して不正使用を行わせないようにする。

【0028】尚、上記の実施例は4つのネットワークを例にとるものであったが、ネットワークの数は必要に応じて適宜に設けられる。また、セキュリティ・サーバを4つのネットワークに対し共通に設けているが、ネットワークの数が増加した場合には、複数のネットワーク単位に共通に1つのセキュリティ・サーバを設け、複数設けられたセキュリティ・サーバ相互間でネットワークすることで、全体的なセキュリティ・サーバとしての機能を実現してもよい。

【0029】

【発明の効果】以上説明してきたように本発明によれば、各ネットワークのホストコンピュータに対し共通にセキュリティ・サーバを設けたことで、複数のホストコンピュータを経由してログインしてきたユーザ端末に対し、各ネットワークのホストコンピュータ間の独立を保ちながら、発信元となったユーザ端末を認識することができ、複数のネットワークを経由することで、不正使用を行おうとしても、不正使用を行っている発信元が追跡されることで、不正使用を確実に把握でき、広域ネットワークのセキュリティを大幅に強化することができる。

【図面の簡単な説明】

【図1】本発明の原理説明図

【図2】本発明の実施例を示したブロック図

【図3】本発明のセキュリティ処理のフローチャート

【図4】従来装置のブロック図

【図5】不正ログインに対する問題の説明図

【符号の説明】

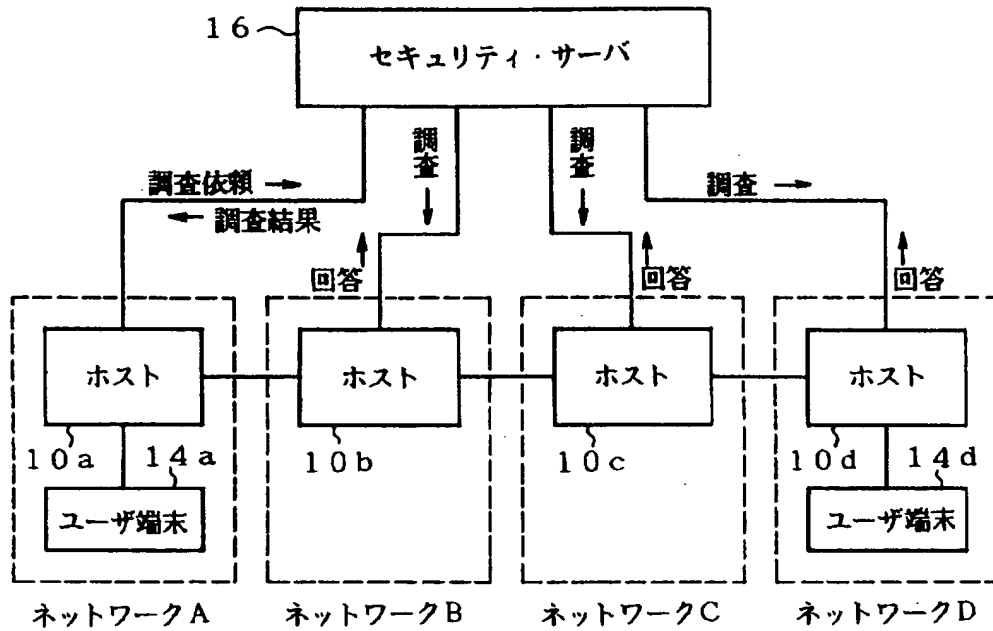
10a～10d：ホストコンピュータ

12：通信回線

14a, 14d：ユーザ端末

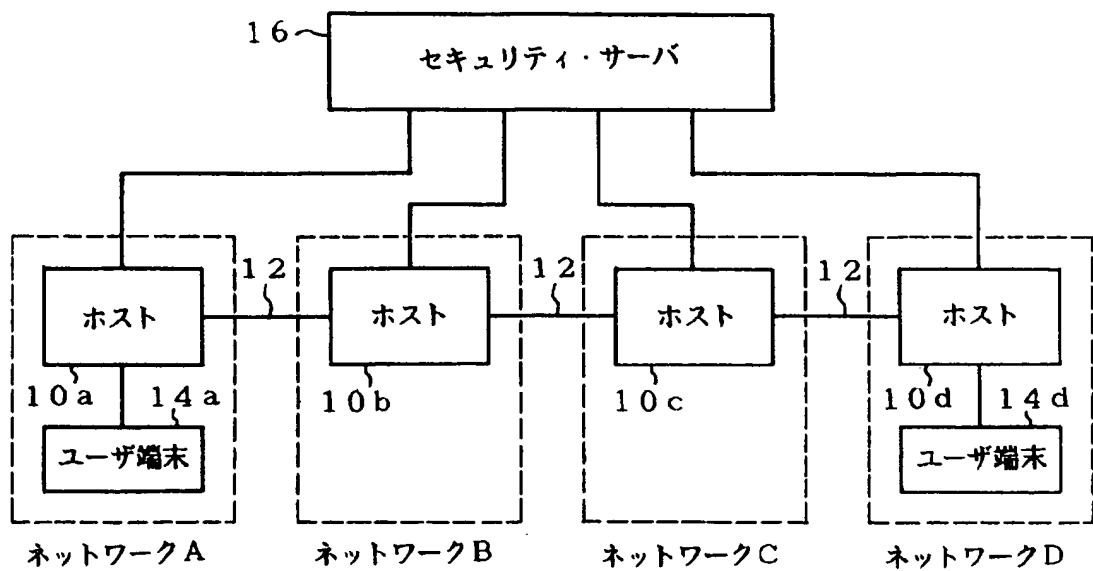
【図1】

本発明の原理説明図



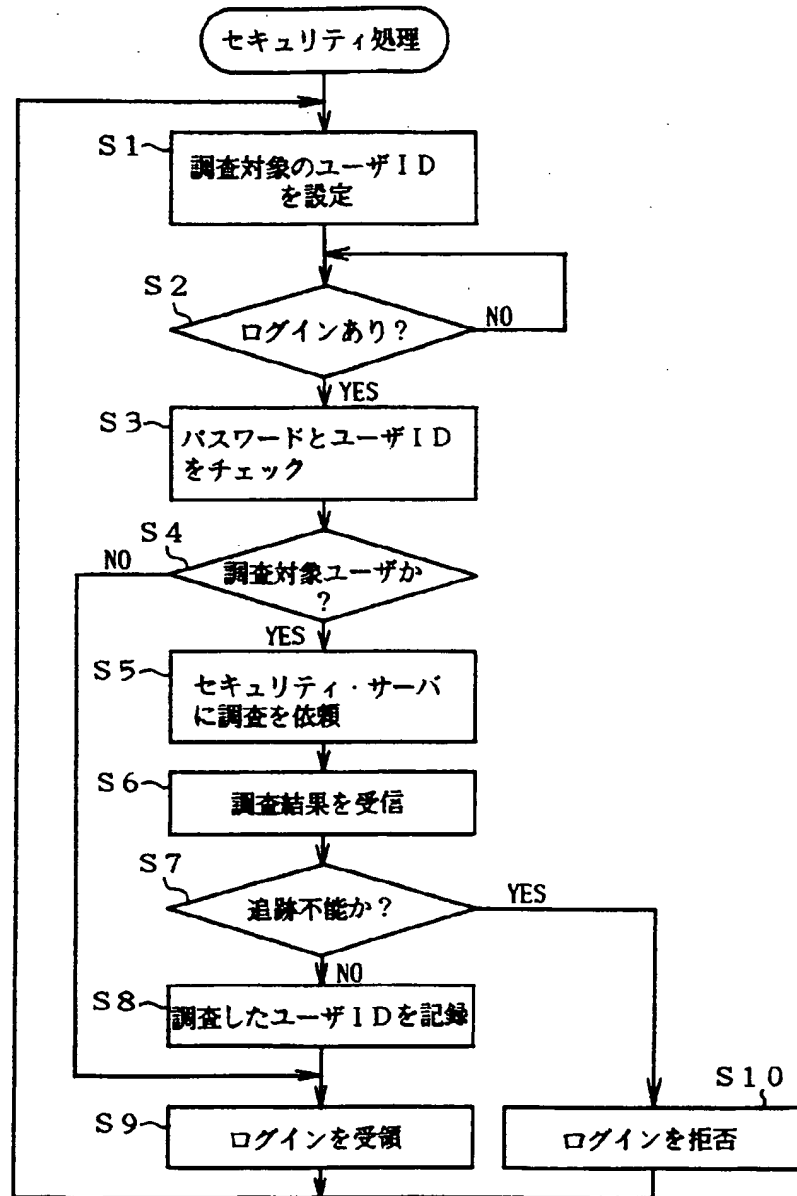
【図2】

本発明の実施例を示したブロック図



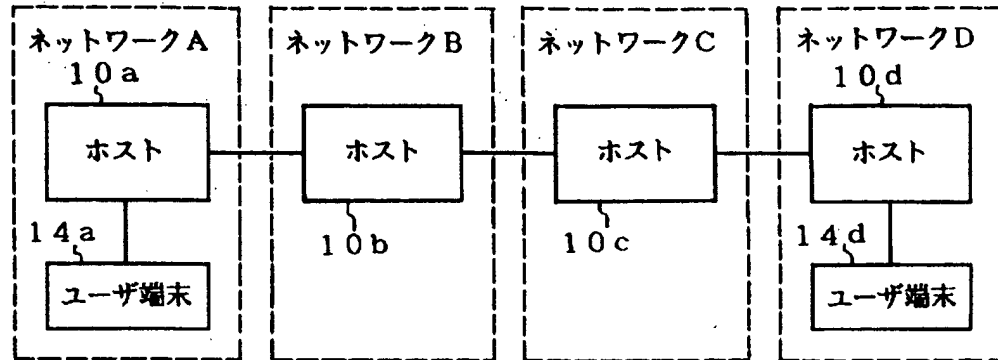
【図 3】

本発明のセキュリティ処理のフローチャート



【図4】

従来装置のブロック図



【図5】

不正ログインに対する問題の説明図

